DE030274 EP
IB/04/51260

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03102410.2 ✓

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03102410.2
Demande no:

Anmeldetag:
Date of filing: 01.08.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Konfiguration einer Netzwerkverbindung

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

Konfiguration einer Netzwerkverbindung

Die Erfindung betrifft ein netzwerkfähiges Gerät, ein Verfahren zur Zuordnung eines solchen Gerätes zu einem Netzwerk und ein Verfahren zur Konfiguration einer Kommunikationsverbindung zwischen einem solchen Gerät und einem Netzwerk.

Bei dem Einbringen eines neuen netzwerkfähigen Gerätes in ein bestehendes drahtloses Netzwerk besteht das Problem, dass das neue Gerät auf Grund der in der Regel ungerichteten, breit gestreuten drahtlosen Kommunikation mehrere verschiedene Netzwerke funktechnisch erreicht und unter diesen das gewünschte Netzwerk richtig auswählen muss. Beispielsweise kann ein tragbarer Computer, der in ein drahtloses Heimnetzwerk eingebunden werden soll, auch in der Reichweite des Netzwerkes einer Nachbarwohnung liegen, sodass während der Herstellung der Kommunikationsverbindung eine Auswahl der richtigen Zuordnung erforderlich ist. Zwar ist es bekannt, alle Geräte eines Netzwerkes durch eine gemeinsame Kennung, einen sogenannten Netzwerkidentifikator, zu kennzeichnen; in der Regel ist dieser Netzwerkidentifikator einem neu einzubringenden Gerät jedoch gerade nicht bekannt und muss daher erst umständlich eingegeben werden. Ähnliche Probleme treten auch bei drahtgebundenen Netzwerken auf, bei denen das zur Kommunikation verwendete Drahtsystem für verschiedene Nutzer offen ist, also z.B. bei Bussystemen sowie insbesondere bei der Verwendung des Stromversorgungsnetzes zur Datenkommunikation ("powerline").

Ferner besteht bei drahtlosen oder offenen drahtgebundenen Netzwerken die Notwendigkeit, die Kommunikation unter den Geräten gegen ein unberechtigtes Abhören zu sichern. Hierzu ist es erforderlich, dass alle Geräte des Netzwerkes einen gemeinsamen Schlüssel, das heißt eine nur ihnen bekannte geheime Information besitzen. Bei der Einbringung eines neuen Gerätes in ein Netzwerk besteht diesbezüglich wiederum das Problem, wie das neue Gerät auf sicherem Wege in Besitz des genannten Schlüssels kommt.

Aus der JP-2001 186123 A ist ein drahtloses netzwerkfähiges Gerät bekannt, bei welchem mit Hilfe eines Sensors aus dem Fingerabdruck eines Benutzers eine persönliche Identifikationsnummer (PIN) abgeleitet wird, mit deren Hilfe dann der gesamte Datenaustausch mit anderen Geräten eines Netzwerkes verschlüsselt wird.

Vor diesem Hintergrund war es eine Aufgabe der vorliegenden Erfindung, Mittel zur Konfiguration einer neuen Netzwerkverbindung bereitzustellen, mit denen insbesondere eine nutzerfreundliche richtige Zuordnung des neuen Gerätes sowie vorzugsweise auch eine Sicherung des Datenverkehrs möglich ist.

Diese Aufgabe wird durch ein netzwerkfähiges Gerät mit den Merkmalen des Anspruchs 1 sowie durch Verfahren mit den Merkmalen der Ansprüche 6 und 7 gelöst. Vorteilhafte Ausgestaltungen sind in den Unteransprüchen enthalten.

Das erfindungsgemäße netzwerkfähige Gerät, bei dem es sich zum Beispiel um einen tragbaren Computer, um eine Videokamera, um ein Audiogerät, um ein TV-Gerät, um ein Mobiltelefon oder dergleichen handeln kann, enthält die folgenden beiden Komponenten:

- Ein Biometriemodul zur Erfassung biometrischer Daten eines Benutzers. Derartige Biometriemodule sind in verschiedenen Ausführungsformen zur Erfassung unterschiedlicher biometrischer Charakteristika (Fingerabdruck, Stimme, DNA etc.) bekannt und dadurch gekennzeichnet, dass sie für einen menschlichen Benutzer individuell charakteristische Daten ermitteln können.

- Ein Konfigurationsmodul, welches mit dem Biometriemodul gekoppelt und dazu eingerichtet ist, aus vom Biometriemodul bereitgestellten biometrischen Daten eines Benutzers einen eindeutigen Netzwerkidentifikator und/oder einen eindeutigen Initialschlüssel für die verschlüsselte Kommunikation (insbesondere in der Konfigurationsphase) zu einem Zweitgerät zu bestimmen. Vorzugsweise ist dabei auch das Zweitgerät vom Typ des erfindungsgemäßen netzwerkfähigen Gerätes, d.h. mit einem Biometriemodul und einem Konfigurationsmodul ausgestattet.

Das beschriebene netzwerkfähige Gerät kann zum einen biometrische Daten eines Benutzers dazu verwenden, eine Kennung für alle zu einem bestimmten Netzwerk gehörigen Geräte (Netzwerkidentifikator) zu ermitteln. Dabei ist es nicht unbedingt erforderlich, dass der Netzwerkidentifikator geheim gehalten wird. Er kann daher offen oder gegebenenfalls auch verschlüsselt von einem Gerät an ein anderes mitgeteilt werden, damit beide Geräte entscheiden können, ob sie zum selben Netzwerk gehören oder nicht. Durch die Ableitung eines Netzwerkidentifikators aus biometrischen Daten eines Benutzers ist insbesondere ein komfortables Verwalten eines Heimnetzwerkes möglich. Ein solches Heimnetzwerk ist nämlich in der Regel dadurch gekennzeichnet, dass (nur) ein bestimmter Benutzer Zugang zu allen zugehörigen Geräten des Netzwerkes hat. Er kann daher insbesondere seine biometrischen Daten, beispielsweise einen Fingerabdruck, an allen Geräten eingeben, sodass diese hieraus einen Netzwerkidentifikator ableiten können. Wenn ein neues Gerät in das bestehende Netzwerk eingebunden werden soll, braucht der Benutzer lediglich auch diesem Gerät seine biometrischen Daten bereitzustellen, woraus das Konfigurationsmodul des Gerätes den Netzwerkidentifikator ermittelt. Das Gerät ist daher anschließend in der Lage, sich in das „richtige" Heimnetzwerk des Benutzers einzubinden, und zwar auch dann, wenn es funktechnisch auch in der Reichweite anderer Netzwerke liegen sollte.

Zusätzlich oder alternativ kann das Konfigurationsmodul auch aus den biometrischen Daten des Benutzers einen "Initialschlüssel" bestimmen, mit dessen Hilfe eine gesicherte (weil verschlüsselte) Kommunikation zwischen Geräten des Heimnetzwerkes von Beginn an gewährleistet wird. Ein unberechtigt erfolgendes Abhören der Kommunikation während der Konfiguration ist daher unschädlich, da der Abhörer nicht die ausgetauschten Informationen entschlüsseln kann. Auch hier ist wiederum von Vorteil, dass der Konfigurationsschlüssel in besonders einfacher Weise den Geräten eines Heimnetzwerkes bereitgestellt werden kann, ohne dass der Nutzer hierfür technisches Hintergrundwissen benötigt oder komplizierte Eingabeprozeduren durchführen muss.

Weiterhin ist das netzwerkfähige Gerät vorzugsweise dazu eingerichtet, die vom Biometriemodul erfassten biometrischen Daten eines Benutzers nach deren Verwendung durch das Konfigurationsmodul wieder zu löschen. Nur die abgeleiteten Netzwerkidentifikatoren oder Schlüssel bleiben gespeichert. Auf diese Weise wird sichergestellt, dass die biometrischen Daten nicht länger gespeichert werden, als dies für die zugrundeliegende Aufgabe erforderlich ist. Daher ist ein Missbrauch dieser Daten ausgeschlossen, wenn die zugehörigen Geräte zum Beispiel durch einen Verkauf in den Besitz Dritter gelangen.

Gemäß einer anderen Weiterbildung der Erfindung ist das Konfigurationsmodul dazu eingerichtet, eine Liste von biometrischen Daten und/oder hieraus abgeleiteten Daten (z.B. Netzwerkidentifikatoren) zu verwalten, um beispielsweise mehreren Benutzern die Konfiguration des Netzwerkes und seiner Komponenten zu ermöglichen. Auf diese Weise ist es möglich, mehreren Benutzern parallel die Konfiguration des Netzwerkes und seiner Komponenten zu ermöglichen. Dabei kann zum Beispiel ein neues Gerät in das Netzwerk eingebunden werden, wenn ihm die biometrischen Daten eines der Benutzer aus der Nutzergruppe zur Verfügung gestellt werden, sodass der hieraus abgeleitete Netzwerkidentifikator in der genannten Liste enthalten ist.

Wie bereits erwähnt wurde, kann die Kommunikation zwischen dem Gerät und dem Zweitgerät drahtlos oder drahtgebunden erfolgen, wobei eine drahtgebundene Kommunikation insbesondere über ein Stromversorgungsnetz stattfinden kann.

Die Erfindung betrifft ferner ein Verfahren zur Zuordnung eines netzwerkfähigen Gerätes zu einem bestimmten Netzwerk, beispielsweise das Einloggen eines tragbaren Computers in eines von mehreren in Funkreichweite liegenden Heimnetzwerken. Bei dem Verfahren werden biometrische Daten eines Nutzers sowohl vom Gerät als auch vom Netzwerk erfasst, und aus den Daten wird ein Netzwerkidentifikator abgeleitet. Die zu einem bestimmten Netzwerk gehörenden Geräte werden somit dadurch ausgezeichnet, dass ein bestimmter Benutzer all diesen Geräten seine biometrischen Daten zum Ein-

lesen und Ableiten eines eindeutigen Netzwerkidentifikators bereitstellt. Das Verfahren eignet sich daher insbesondere für die Lösung des Zuordnungsproblems bei Heimnetzwerken, bei denen typischerweise ein Nutzer Zugriff auf alle Komponenten hat.

Die Erfindung betrifft ferner ein Verfahren zur Konfiguration einer Kommunikationsverbindung zwischen einem netzwerkfähigen Gerät und einem Netzwerk. Dabei werden wiederum biometrische Daten eines Nutzers sowohl vom Gerät als auch vom Netzwerk erfasst, und aus den erfassten Daten wird ein Schlüssel für eine gesicherte Kommunikation während der Konfiguration generiert. Auch dieses Verfahren ist insbesondere für Heimnetzwerke geeignet, wo es eine abhörsichere Konfiguration ermöglicht. Der Benutzer benötigt diesbezüglich keine vertieften technischen Kenntnisse, sondern die erforderliche Prozedur, die z.B. lediglich ein Berühren des neuen zum Netzwerk gehörenden Gerätes erfordert, ist im Gegensatz sogar für technische Laien plausibel.

Im Folgenden wird die Erfindung mit Hilfe der beigefügten Figur beispielhaft erläutert. Die einzige Abbildung zeigt schematisch ein erfindungsgemäßes netzwerkfähiges Gerät während der Konfiguration einer Kommunikationsverbindung zu einem Heimnetzwerk.

In der Figur sind mit den Buchstaben A und B zwei verschiedene Heimnetzwerke bezeichnet, in denen jeweils Geräte wie beispielsweise Videorecorder, TV-Geräte, Stereoanlagen, Computer etc., die zu einem bestimmten Haushalt gehören, drahtlos oder drahtgebunden miteinander gekoppelt sind. Als drahtgebundene Verbindung kommt dabei insbesondere ein sogenannter powerline Anschluss in Frage, bei welchem die Datenkommunikation über das Stromversorgungsnetz erfolgt.

Bei der zugrundeliegenden Situation sollen die beiden Netzwerke A, B eine überlappende Funkreichweite haben, zum Beispiel weil sie in Nachbarwohnungen angeordnet sind (eine solche Überlappung ergäbe sich auch bei einer powerline Kommunikation). Die überlappenden Reichweiten führen zu einem Problem, wenn ein neues netzwerkfähiges Gerät 2 in das Heimnetzwerk A des Benutzers 1 eingebunden werden soll. Ohne

zusätzliche Informationen bzw. eine Vorkonfiguration kann das Gerät 2 nämlich nicht entscheiden, ob es gerade eine Verbindung zum „richtigen" Netzwerk A oder zum „falschen" Netzwerk B hat.

Um dieses Zugehörigkeitsproblem in einfacher und nutzerfreundlicher Weise zu lösen, ist das Gerät 2 mit einem Biometriemodul 3 und einem Konfigurationsmodul 4 versehen. Das Biometriemodul 3 ist dazu eingerichtet, biometrische Daten eines Nutzers 1 zu erfassen. Bei diesen biometrischen Daten kann es sich beispielsweise um den Fingerabdruck, die Sprache, die Ohrform, die Handform, um DNA-Spuren, um einen Handdruck, um eine nach Geschwindigkeit und Druck differenzierte Unterschrift oder dergleichen handeln, wobei jeweils geeignete Sensoren zur Erfassung der genannten Größen im Stand der Technik bekannt sind. Das Biometriemodul 3 sollte dabei bestimmten Sicherheitsstandards genügen, um zum Beispiel nicht das Abspielen biometrischer Daten und ihre Speicherung für andere als die gewünschten Zwecke zu ermöglichen. Das Biometriemodul 3 sollte z.B. von einer unabhängigen Autorität zertifiziert und zur Verhinderung von Manipulationen versiegelt sein. Ferner sollte die Integrität des Biometriemoduls 3 überwacht werden und von anderen Einheiten im Netzwerk überprüfbar sein.

Die erfassten biometrischen Daten werden an das Konfigurationsmodul 4 weitergeleitet, welches hieraus einen Netzwerkidentifikator und vorzugsweise auch einen Konfigurationsschlüssel ableitet, wobei diese Größen anschließend zur Lösung des Zugehörigkeitsproblems sowie für eine gesicherte Konfigurationsprozedur verwendet werden können. Dabei ist lediglich vorauszusetzen, dass der Nutzer 1 bei den Geräten des Netzwerkes A, die eine drahtlose Kommunikationsverbindung eingehen können (zum Beispiel Zugangspunkte mit verkabelten Verbindungen zu sonstigen Geräten) ebenfalls seine biometrischen Daten bei deren (früheren) Konfiguration eingegeben hat oder nun eingibt. Die Geräte des Netzwerkes A sind somit vorzugsweise ähnlich ausgestaltet wie das Gerät 2.

Da der Benutzer 1 Zugang zu seinem Heimnetzwerk A sowie dem einzubindenden Gerät 2, nicht jedoch zum Heimnetzwerk B hat, lässt sich durch die Verwendung des aus seinen biometrischen Daten abgeleiteten Netzwerkidentifikators das Zugehörigkeitsproblem lösen. Dass heißt, dass das Konfigurationsmodul 4 bei einer drahtlosen Kommunikation über eine Schnittstelle 5 erkennen kann, ob es mit dem „richtigen", zum Nutzer 1 gehörenden Netzwerk A kommuniziert.

Im Rahmen einer Verwaltung der auf biometrischen Daten basierenden Schlüssel muss ein einfaches, unbeabsichtigtes oder unautorisiertes Überschreiben eines hinterlegten Schlüssels verhindert werden. Dies kann zum Beispiel dadurch erreicht werden, dass für die Eingabe neuer biometrischer Daten (zum Beispiel Abdrücke anderer Finger eines Benutzers 1, Fingerabdrücke von anderen Familienmitgliedern, von Gästen oder von unberechtigten Personen) eine zweite oder wiederholte Neueingabe nach einem definierten Zeitraum der Ersteingabe (zum Beispiel eine Stunde oder ein Tag) erforderlich ist, wobei nur der autorisierte Benutzer 1 die richtigen Zeitabstände kennt. Ebenso könnte die Neueingabe biometrischer Daten und das Ersetzen der bestehenden Schlüssel erfordern, dass zur Bestätigung die ursprünglichen biometrischen Daten eingegeben werden müssen.

Des Weiteren ist darauf zu achten, dass die auf den biometrischen Daten des Benutzers 1 beruhenden Informationen einschließlich der biometrischen Daten selbst löschbar sein müssen, damit der Benutzer 1 das Gerät 2 gegebenenfalls entsorgen oder verkaufen kann, ohne dabei persönliche Daten aus der Hand zu geben. Da die biometrischen Daten nur während der Initialisierungsphase einer sicheren Autokonfiguration zur Lösung des Zugehörigkeitsproblems sowie zur Vereinbarung einer abhörsicheren Datenkommunikation erforderlich sind, werden sie vorzugsweise unmittelbar nach ihrer Verwendung gelöscht. Nur die hieraus abgeleiteten Schlüsseldatensätze und Netzwerkinformationen werden dauerhaft gespeichert. Wenn der Benutzer 1 zu einem späteren Zeitpunkt ein neues Gerät in das existierende Netzwerk einbringen will, gibt er seine biometrischen Daten am neuen Gerät ein, worauf das Konfigurationsmodul den eindeutigen Netzwerkidentifikator und/oder den eindeutigen Initialschlüssel ableitet.

Dabei ist es nicht erforderlich, den Initialschlüssel dauerhaft zu verwenden. Vielmehr besteht die Möglichkeit, den Initialschlüssel nur zur Vereinbarung von weiteren Kryptographieschlüsseln zu verwenden. Dass heißt der auf den biometrischen Daten beruhrende Initialschlüssel wird nur zum Schutz eines nachfolgenden Schlüsselaustauschs verwendet, während alle weitere Kommunikation durch die neuen (Sitzungs-)Schlüssel geschützt wird.

Weiterhin kann auch für mehrere Nutzer (zum Beispiel Familienmitglieder) ein Zugriff auf Konfigurationsfunktionen des Netzwerkes eingerichtet werden. Zu diesem Zweck ist eine Liste von biometrischen Daten oder hieraus abgeleiteten Größen, zum Beispiel Netzwerkidentifikatoren, für die autorisierten Nutzer der genannten Gruppe bereitzustellen. In einer Initialisierungsphase wird dabei eine Anzahl zulässiger Fingerabdrücke (als Beispiel biometrischer Daten) einem oder mehreren Geräten des Netzwerkes A präsentiert. Aus diesen Fingerabdrücken wird dann eine korrespondierende Liste an abgeleiteten Daten erzeugt. Wann immer später ein neues Gerät 2 in das Netzwerk A eingebracht werden soll, reicht es für die Akzeptanz des neuen Gerätes aus, wenn diesem einer der autorisierten Fingerabdrücke bereitgestellt wird. Das für die Netzwerkkommunikation verwendete gemeinsame Geheimnis wird dann nur indirekt abgeleitet, zum Beispiel aus einem primären Fingerabdruck (der zum Beispiel der erste dem Netzwerk präsentierte Fingerabdruck sein kann). Weiterhin können zwischen den verschiedenen Benutzern und ihren entsprechenden biometrischen Daten verschiedene Prioritäten definiert werden.

BEZUGSZEICHENLISTE

A, B Heimnetzwerke

1 Benutzer

2 netzwerkfähiges Gerät

3 Biometriemodul

4 Konfigurationsmodul

5 drahtlose Schnittstelle

PATENTANSPRÜCHE

1. Netzwerkfähiges Gerät (2), enthaltend
   - ein Biometriemodul (3) zur Erfassung biometrischer Daten eines Benutzers (1);
   - ein Konfigurationsmodul (4), welches dazu eingerichtet ist, aus vom Biometriemodul (3) bereitgestellten biometrischen Daten einen eindeutigen Netzwerkidentifikator und/oder einen eindeutigen Initialschlüssel für die verschlüsselte Kommunikation (insbesondere während der Konfigurationsphase) zu einem Zweitgerät zu bestimmen.

2. Gerät nach Anspruch 1,
dadurch gekennzeichnet,
dass es dazu eingerichtet ist, die biometrischen Daten eines Benutzers (1) nach deren Verwendung durch das Konfigurationsmodul (4) zu löschen.

3. Gerät nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die Kommunikation mit dem Zweitgerät drahtlos oder drahtgebunden, insbesondere über ein Stromversorgungsnetz erfolgt.

4. Gerät nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass das Konfigurationsmodul dazu eingerichtet ist, eine Liste von biometrischen Daten und/oder hieraus abgeleiteten Daten für verschiedene Benutzer (1) einer autorisierten Nutzergruppe zu verwalten.

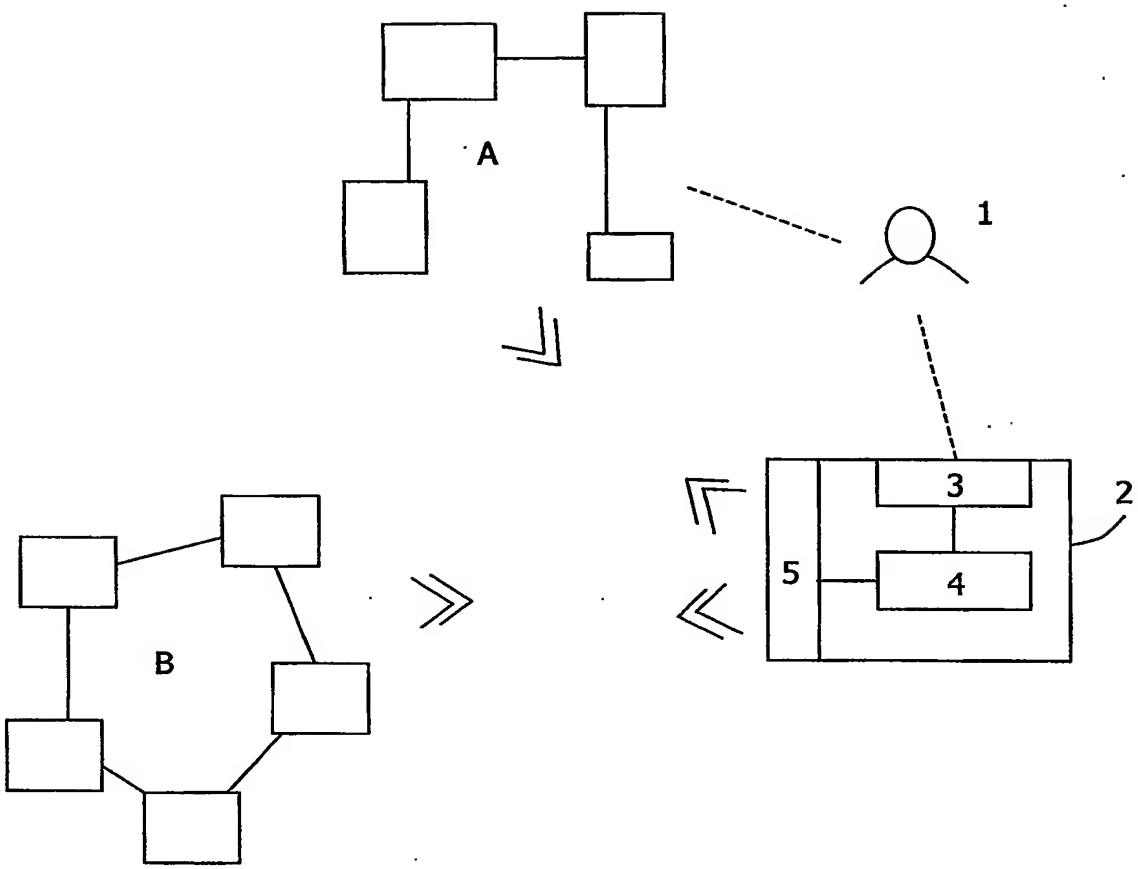
5. Verfahren zur Zuordnung eines netzwerkfähigen Gerätes (2) zu einem Netzwerk (A), wobei biometrische Daten eines Nutzers (1) vom Gerät (2) erfasst werden und aus diesen ein eindeutiger Netzwerkidentifikator abgeleitet wird, der im Netzwerk (A) aus früheren und/oder gleichzeitigen Eingaben derselben biometrischen Daten bekannt ist und benutzt wird..

6. Verfahren zur Konfiguration einer Kommunikationsverbindung zwischen einem netzwerkfähigen Gerät (2) und einem Netzwerk (A), wobei biometrische Daten eines Nutzers (1) vom Gerät erfasst werden und aus diesen ein eindeutiger Initialschlüssel abgeleitet wird, der im Netzwerk (A) aus früheren und/oder gleichzeitigen Eingaben derselben biometrischen Daten bekannt ist und eine gesicherte Kommunikation (insbesondere in der Konfigurationsphase) benutzt wird.

ZUSAMMENFASSUNG

Konfiguration einer Netzwerkverbindung

Die Erfindung betrifft ein Verfahren zur Einbringung eines netzwerkfähigen Gerätes (2) in ein existierendes Netzwerk (A), wobei ein Benutzer (1) dem Gerät (2) sowie Geräten des Netzwerkes (A) über ein Biometriemodul (3) charakteristische biometrische Daten bereitstellt. Aus den biometrischen Daten kann dann ein Netzwerkidentifikator und/oder ein Konfigurationsschlüssel abgeleitet werden. Der Netzwerkidentifikator kann sicherstellen, dass das neue Gerät (2) eine richtige Zuordnung zum gewünschten Netzwerk (A) auch dann vornimmt, wenn es in seiner Reichweite noch andere Netzwerke (B) gibt. Der Konfigurationsschlüssel kann für eine Sicherung der während der Konfigurationsphase ausgetauschten Informationen gegen ein Abhören verwendet werden.


A
1
3
2
5
4
B